Amendments to the Claims

In this Preliminary Amendment, claims 1-11 are being cancelled. Claims 12-19 are being added. The following listing of claims replaces all previous versions of the claims in the application.

Listing of Claims

1-11 (canceled)

12. (New) A method for preventing intrusions to a computer system, comprising:

using a network-based appliance to intercept data packets;

deciding whether to forward the intercepted packets or whether to route the intercepted packets to a virtual proxy;

performing TCP or UDP processing on the intercepted packets before routing them to the virtual proxy;

using the virtual proxy to analyze the packets that have been routed to the virtual proxy to detect intrusions; and

when the virtual proxy detects an attack or violation in the packets, using the virtual proxy to direct a transport layer to modify the packets.

13. (New) The method defined in claim 12 wherein using the virtual proxy to direct the transport layer to modify the packets further comprises:

modifying data in the packets at specified locations.

14. (New) The method defined in claim 12 further comprising using the virtual proxy to direct the transport layer to remove data from the packets when the virtual proxy detects an attack or violation.

15. (New) The method defined in claim 12, wherein the virtual proxy directs the transport layer to modify the packets using packet stream modification requests, the method further comprising sending the packet stream modification requests from an active network-based appliance to a standby network-based appliance to support fault tolerance.

16. (New) A method for building and using a customized processing engine that prevents intrusions into a computer system, comprising:

creating processing procedures that capture violations for vulnerabilities and exposures;

dynamically loading libraries of the processing procedures into a network-based appliance at run time, wherein the libraries of processing procedures include functions for adding the processing procedures to the customized processing engine;

using the functions to add the processing procedures to the customized processing engine; and

using the customized processing engine to prevent intrusions into the computer system.

17. (New) The method defined in claim 16 further comprising:

updating the customized processing engine to create a new customized processing engine by dynamically loading the libraries of processing procedures for the new customized processing engine.

18. (New) The method defined in claim 17 further comprising:

using the customized processing engine to handle existing application sessions and using the new customized processing engine to handle new application sessions.

19. (New) The method defined in claim 16 further comprising:

using sequence numbers to dictate which order the libraries of processing procedures are loaded.